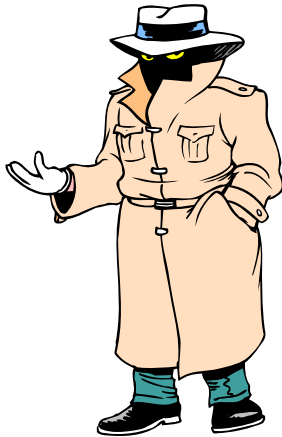


ID THEFT:

WHAT TO DO IF IT HAPPENS TO YOU



WHAT IS ID THEFT?

Identity theft is the unlawful use of your personal information (credit card numbers, your name, address, social security number, business tax ID number, etc). Identity thieves are just that – they impersonate their victims and use other's information.

HOW DOES IT HAPPEN?

Thieves get information in a variety of ways:

- ♣ Asking!
- ♣ Lost or stolen paycheck stubs
- ♣ Preapproved offers
- ♣ Bogus bank/IRS forms returned to them by unsuspecting consumers
- ♣ Phishing/bogus Websites and e-mails
- ♣ Discarded, stolen or duplicate checks
- ♣ Address change forms
- ♣ Passports
- ♣ Registration information
- ♣ Stolen ATM/check/credit cards

HOW TO MINIMIZE YOUR RISK

- ♣ Shred unnecessary documents and account information and discard old receipts, files, and records after a few years.
- ♣ Check your credit report at least once a year for inaccuracies, new accounts, and changes of name or address.
- ♣ Don't give your information to unfamiliar people or businesses – no matter how official they seem.
- ♣ Ask inquirers about the information they need: why do they need it? What will they do with it and how will they protect it? With whom will they share?
- ♣ Don't use your private information as identifiers. (Pin numbers, etc. Ask if you can set your own pass code instead.

WHAT TO DO IF YOUR IDENTITY IS STOLEN

- ✚ Contact the fraud departments of the three major credit bureaus.
- ✚ Contact local law enforcement and get a written report of the theft.
- ✚ Contact your creditors and notify them of any accounts that have been or may be tampered with or opened fraudulently.
- ✚ Contact your creditors and tell them what has happened; you will need a police report or similar documentation. Have them place fraud alerts on your accounts.
- ✚ Check with your bank and stop payment on any checks or accounts that have been tampered with. If opening a new account, insist on password-only access.
- ✚ Report any tampering with investments to your broker or account manager and the



- Securities and Exchange Commission.
- ✚ Contact your telephone, cell phone service, or utilities provider to cancel the account or service if someone has established use in your name. Have them place an alert on your file, if possible.
- ✚ Report fraud to the Social Security Administration Fraud Hotline 800.269.0271 or oig.hotline@ssa.gov
- ✚ When talking to the store, agency, company, or organization where your information was used, do some detective work: how did they open the account? When? Where?
- ✚ Document everything, and try to get all information in writing – paper trails are very helpful in catching identity thieves and getting back your good name
- ✚ Notify and file a complaint with the FTC www.consumer.gov/idtheft or 1.877.IDTHEFT

For more information:
Visit SCDCA's Website at www.scconsumer.gov
or
contact
Sherry Gore King, Director of Educational Services
800. 922.1594 (toll-free in SC)
803.734.4200
www.ftc.gov
www.consumer.gov/idtheft
www.idtheftcenter.org
www.usdoj.gov/criminal/fraud/idtheft.html